APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/090,136	03/01/2002	Jiewen Liu	42390P11398	3593

			EXAMINER
8791	7590	05/30/2006	HASHEM, LISA

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

ART UNIT	PAPER NUMBER
2614	

DATE MAILED: 05/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
	10/090,136	LIU ET AL.
Office Action Summary	Examiner	Art Unit	
	Lisa Hashem	2614	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>06 March 2006</u>.

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-34</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-34</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

FINAL DETAILED ACTION

Claim Rejections - 35 USC § 102

1.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed
> in the United States before the invention by the applicant for patent or (2) a patent granted on an application for
> patent by another filed in the United States before the invention by the applicant for patent, except that an
> international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this
> subsection of an application filed in the United States only if the international application designated the United
> States and was published under Article 21(2) of such treaty in the English language.

2.   Claims 1-34 are rejected under 35 U.S.C. 102(e) as being clearly anticipated over U.S.

Patent No. 6,732,176 by Stewart et al, hereinafter Stewart.

Regarding claim 1, Stewart discloses a method comprising:

broadcasting a synchronization signal from a wireless access point device (Fig. 1, 120) indicating

one of a plurality of modes of operation for the access point (col. 6, lines 21-25; col. 11, lines 12-

16),

the plurality of modes of operation including a private mode of operation for authorized devices

(or portable computing device (PCDs)) (col. 10, line 64 – col. 11, line 16; col. 15, line 56 – col.

16, line 14) and

a public mode of operation for authorized or non-authorized devices (col. 12, lines 11-29; col.

15, lines 29-39; col. 16, lines 15-37);

broadcasting available public network services if the mode of operation is the public mode of

operation (e.g. advertising on the local LAN) (col. 12, lines 11-29);

receiving a request for establishment of a connection from a non-authorized mobile device in

response to the broadcast of the synchronization signal for the public mode of operation (col. 11,

lines 12-16; col. 15, lines 29-47); and

establishing a connection between the non-authorized mobile device and the access point device

(col. 12, lines 11-29; col. 15, lines 29-47; col. 16, lines 15-37);

wherein establishing a connection in the private mode comprises use of a secure authentication

process (col. 6, lines 15-28; col. 10, lines 53-63; col. 11, lines 54-65; col. 14, line 57 – col. 15,

line 5), and

 wherein establishing a connection in the public mode comprises use of a registration process

(col. 11, line 66 – col. 12, line 10; col. 15, lines 29-47).

Regarding claim 2, the method of claim 1 mentioned above, wherein Stewart further

discloses:

receiving a request for connection establishment from the non-authorized mobile device for

access to a selected network service of the available network services; and

allowing the non-authorized mobile device access to the selected network service

(col. 11, lines 12-16; col. 12, lines 11-29; col. 14, lines 1-20; col. 15, lines 29-47; col. 16, lines

15-37).

Regarding claim 3, the method of claim 1 mentioned above, wherein Stewart further

discloses the available network services includes free public network services (e.g. advertising

on the local LAN) (col. 12, lines 11-29).

Regarding claim 4, the method of claim 1 mentioned above, wherein Stewart further discloses the available network services includes pay-per-use public network services (col. 14, lines 21-27; col. 14, line 57 – col. 15, line 5; col. 15, lines 29-47).

Regarding claim 5, the method of claim 4 mentioned above, wherein Stewart further discloses: providing a form of payment for a pay-per-use network service (col. 11, line 66 – col. 12, line 10).

Regarding claim 6, the method of claim 5 mentioned above, wherein Stewart further discloses the form of payment is a credit card number (col. 11, line 66 – col. 12, line 10).

Regarding claim 7, the method of claim 5 mentioned above, wherein Stewart further discloses the form of payment is a prepaid payment number (col. 11, lines 28-53).

Regarding claim 8, the method of claim 5 mentioned above, wherein Stewart further discloses: providing a secure transmission of information between the non-authorized mobile device and the access point device (col. 6, lines 29-39; col. 16, lines 15-37).

Regarding claim 9, the method of claim 5 mentioned above, wherein Stewart further discloses: sending payment information from the non-authorized mobile device to the access point device wirelessly (col. 11, line 66 – col. 12, line 10).

Regarding claim 10, the method of claim 5 mentioned above, wherein Stewart further discloses:

inherently validating the payment information provided by the non-authorized mobile device; and

providing the validation results to the non-authorized mobile device (col. 11, lines 28-53; col. 11, line 66 – col. 12, line 10).

Regarding claim 11, the method of claim 10 mentioned above, wherein Stewart further discloses:

inherently establishing a connection between the non-authorized mobile device and a selected network service only if payment validation successful (col. 11, lines 28-53; col. 11, line 66 – col. 12, line 10).

Regarding 12, the method of claim 11 mentioned above, wherein Stewart further discloses:

if a payment for the non-authorized mobile device expires,

inherently disconnecting the non-authorized mobile device from a selected network service, of the available network services (col. 11, lines 28-53; col. 11, line 66 – col. 12, line 10).

Regarding claim 13, the method of claim 1 mentioned above, wherein Stewart further discloses: performing data exchanges between the non-authorized mobile device and a selected network service of the available network services, through the access point (col. 13, lines 43-47; col. 13, lines 53-61).

Regarding claim 14, the method of claim 1 mentioned above, wherein Stewart further discloses: inherently disconnecting the non-authorized mobile device from the access point device to terminate access to the available network services (e.g. the mobile device is finished using the services) (col. 5, lines 36-47).

Regarding claim 15, the method of claim 1 mentioned above, wherein Stewart further discloses the establishment of the connection uses an authentication procedure (e.g. digital certification) provided in Electrical and Electronics Engineers (IEEE) Standard 802.11 Specification or its supplements (col. 1, lines 44-53; col. 5, lines 8-11; col. 5, lines 20-24; col. 6,

lines 21-28; col. 10, lines 53-63; col. 11, lines 59-65; col. 14, lines 35-40; col. 14, line 57 – col.

15, line 1).

Regarding claim 16, a machine-readable medium (Fig. 1, 120) having one or more

instructions for enabling a non-authorized user to wirelessly access a number of network

services, which when executed by a processor (col. 5, lines 36-47; col. 6, lines 29-39; col. 8,

lines 35-49), causes the processor to perform operations comprising:

wirelessly transmitting a synchronization signal indicating one of a plurality of modes of

operation for an access point (col. 6, lines 21-25; col. 11, lines 12-16),

the plurality of modes of operation including a private mode of operation for authorized devices

(or portable computing device (PCDs)) (col. 10, line 64 – col. 11, line 16; col. 15, line 56 – col.

16, line 14) and

a public mode of operation for authorized or non-authorized devices (col. 12, lines 11-29; col.

15, lines 29-39; col. 16, lines 15-37);

wirelessly transmitting available network services if the mode of operation is the public mode of

operation (e.g. advertising on the local LAN) (col. 12, lines 11-29);

receiving a request for connection establishment from a non-authorized user in response to the

transmission of a synchronization signal for the public mode of operation (col. 11, lines 12-16;

col. 15, lines 29-47);

establishing a connection with the non-authorized user (col. 12, lines 11-29; col. 15, lines 29-47;

col. 16, lines 15-37);

receiving a request for access to a selected network service, from among the available network

services, by the non-authorized user; and

providing the non-authorized user access to the selected network service (col. 11, lines 12-16;

col. 12, lines 11-29; col. 15, lines 29-47; col. 16, lines 15-37);

wherein establishing a connection in the private mode comprises use of authentication (e.g.

'providing identification information') and association handshakes (e.g. 'listening', 'answering

queries') (col. 10, line 64 – col. 11, line 16), and

wherein establishing a connection in the public mode comprises use of a registration process

(col. 11, line 66 – col. 12, line 10; col. 15, lines 29-47).

Regarding claims 17-20, 30, and 31, please see the rejections of the method in claims 4,

11, 12, 13, 28, and 29, respectively, to reject the machine-readable medium in claims 17-20, 30,

and 31.

Regarding claim 21, Stewart discloses an apparatus (Fig. 1, 120) comprising:

a transceiver port for wirelessly communicating with mobile devices (col. 5, lines 5-11; col. 6,

lines 29-39);

a network communications port communicatively coupled to the transceiver port, the network

communications port for coupling to a network (col. 5, lines 15-24); and

a control unit inherently coupled to the transceiver port and the network communications port

(col. 8, lines 35-49), the control unit inherently configured to control access from the transceiver

port to the network communications port and provide at least two modes of operation, a first

mode of operation to provide authorized mobile devices private access to the network

communications port (col. 10, line 64 – col. 11, line 16; col. 15, line 56 – col. 16, line 14), and

a second mode of operation to provide authorized and non-authorized mobile devices public

access to the network communications port (col. 12, lines 11-29; col. 15, lines 29-39; col. 16,

lines 15-37),

wherein the control unit is to use the transceiver port to broadcast a synchronization signal

indicating one of the modes of operation and, for the second mode of operation, available

network services, and to receive a response from an unauthorized mobile device in response to

the broadcast of the synchronization signal (col. 6, lines 21-25; col. 11, lines 12-16; col. 15, lines

29-39);

and wherein the control unit is to establish a connection in the private mode through use of

authentication and association handshakes (e.g. 'providing identification information') and

association handshakes (e.g. 'listening', 'answering queries') (col. 10, line 64 – col. 11, line 16),

and

to establish a connection in the public through the use of a registration process (col. 11, line 66 –

col. 12, line 10; col. 15, lines 29-47).

Regarding claim 22, the apparatus of claim 21 mentioned above, wherein Stewart further

discloses any one of the operation modes can be dynamically enabled or disabled (col. 12, lines

11-29; col. 15, lines 29-39; col. 15, line 56 – col. 16, line 14; col. 16, lines 15-37).

Regarding claim 23, the apparatus of claim 21 mentioned above, wherein Stewart further

discloses in the first mode of operation a specific authentication process is requested from the

mobile devices to obtain full network access over the network communications port and in the

second mode of operation no specific authentication process is requested from the mobile

devices to obtain certain network access over the network communications port (col. 12, lines 11-29; col. 15, line 56 – col. 16, line 14).

Regarding claim 24, the apparatus of claim 21 mentioned above, wherein Stewart further discloses the second mode of operation allows the non-authorized mobile devices to obtain public network access through the network communication port (col. 14, lines 1-20).

Regarding claim 25, the apparatus of claim 21 mentioned above, wherein Stewart further discloses the control unit is inherently configured to provide secure services to both authorized and non-authorized mobile devices (col. 12, lines 11-29; col. 15, line 56 – col. 16, line 14).

Regarding claim 26, the apparatus of claim 21 mentioned above, wherein Stewart further discloses the control unit is inherently configured to provide data exchange to both authorized and non-authorized mobile devices utilizing an authorization process (e.g. digital certification) provided in the Electrical and Electronics Engineers (IEEE) 802.11 Standard or its supplements (col. 1, lines 44-53; col. 5, lines 8-11; col. 5, lines 20-24; col. 6, lines 21-28; col. 10, lines 53-63; col. 11, lines 59-65; col. 14, lines 35-40; col. 14, line 57 – col. 15, line 1).

Regarding claim 27, the apparatus of claim 21 mentioned above, wherein Stewart further discloses the control unit is inherently configured to provide a third mode of operation, the third mode of operation provides authorized mobile devices access to the network communications port and non-authorized mobile devices limited access to the network communications port simultaneously (col. 14, lines 1-20; col. 15, line 56 – col. 16, line 14).

Regarding claim 28, the method of claim 1 mentioned above, wherein Stewart further discloses the private mode of operation includes a secure service (e.g. digital certification; secure payment method) as specified in the Electrical and Electronics Engineers (IEEE) Standard

802.11 Specification or its supplements (col. 1, lines 44-53; col. 5, lines 8-11; col. 5, lines 20-24;

col. 6, lines 21-28; col. 10, lines 53-63; col. 10, line 64 – col. 11, line 16; col. 11, line 54 – col.

12, line 46; col. 14, lines 35-40; col. 14, line 57 – col. 15, line 1).

Regarding claim 29, the method of claim 1, wherein Stewart further discloses the

plurality of modes of operation includes a simultaneous mode of operation, the simultaneous

mode of operation providing authorized mobile devices access to private network services and

authorized or non-authorized mobile devices access to public network services simultaneously

via the access point (col. 14, lines 1-20; col. 15, line 56 – col. 16, line 14).

Regarding claim 32, the method of claim 15, wherein Stewart discloses the

establishment of a connection in the private mode comprises use of Secure Service procedures as

specified in IEEE Standard 802.11 Specification or its supplements (e.g. authentication and

encryption; secure payment option) (col. 1, lines 44-53; col. 5, lines 8-11; col. 5, lines 20-24; col.

11, line 66 – col. 12, line 10; col. 14, line 57 – col. 15, line 5); and

the establishment of a connection in the public mode comprises use of Open System procedures

as specified in IEEE Standard 802.11 Specification or its supplements (e.g. identity assertion;

request for authentication and an authentication result) (col. 1, lines 44-53; col. 5, lines 8-11; col.

5, lines 20-24; col. 10, line 64 – col. 11, line 16; col. 11, line 54 – col. 12, line 46).

Regarding claim 33, the machine-readable medium of claim 16, wherein Stewart

discloses the establishment of a connection in the private mode comprises use of Secure Service

procedures as specified in the Electrical and Electronics Engineers (IEEE) Standard 802.11

Specification or its supplements (e.g. authentication and encryption; secure payment option) (col.

1, lines 44-53; col. 5, lines 8-11; col. 5, lines 20-24; col. 11, line 66 – col. 12, line 10; col. 14,

line 57 – col. 15, line 5); and

the establishment of a connection in the public mode comprises use of Open System procedures

as specified in IEEE Standard 802.11 Specification or its supplements (e.g. identity assertion;

request for authentication and an authentication result) (col. 1, lines 44-53; col. 5, lines 8-11; col.

5, lines 20-24; col. 10, line 64 – col. 11, line 16; col. 11, line 54 – col. 12, line 46).

Regarding claim 34, the apparatus of claim 26, wherein Stewart discloses the control unit

is configured to: establish a connection in the private mode through use of Secure Service

procedures as specified in IEEE Standard 802.11 Specification or its supplements (e.g.

authentication and encryption; secure payment option) (col. 1, lines 44-53; col. 5, lines 8-11; col.

5, lines 20-24; col. 11, line 66 – col. 12, line 10; col. 14, line 57 – col. 15, line 5); and

establish a connection in the public mode through use of Open System procedures as specified in

IEEE Standard 802.11 Specification or its supplements (e.g. identity assertion; request for

authentication and an authentication result) (col. 1, lines 44-53; col. 5, lines 8-11; col. 5, lines 20-

24; col. 10, line 64 – col. 11, line 16; col. 11, line 54 – col. 12, line 46).

Response to Arguments

3.   Applicant's arguments with respect to claims 1-34 have been considered but are moot in

view of the new ground(s) of rejection.

4.   Accordingly, this action is **FINAL**.

Conclusion

5.   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure:

- U.S. Patent Application Publication No. 2002/0075844 by Hagen discloses a network

    access server or access point that provides an interface between wireless, mobile

    terminals and a private network; wherein the NAS restricts access by the mobile

    terminals to the private network

6.   Any response to this action should be mailed to:

<div align="center">

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

</div>

Or faxed to:

(571) 273-8300 (for formal communications intended for entry)

Or call:

(571) 272-2600 (for customer service assistance)

7.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Lisa Hashem whose telephone number is (571) 272-7542. The

examiner can normally be reached on M-F 8:30-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Fan Tsang can be reached on (571) 272-7547. Any inquiry of a general nature or

relating to the status of this application or proceeding should be directed to the Group

receptionist whose telephone number is (571) 272-2600.

8.   Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

lh
May 22, 2006

FAN TSANG
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600